September 5, 2007

Federal Trade Commission
Office of the Secretary
Room H-135 (Annex K)
600 Pennsylvania Avenue, NW
Washington, DC 20580

RE: SSNs In The Private Sector – Comment, Project No. P075414

To Whom It May Concern:

The American Financial Services Association (AFSA) welcomes the opportunity to comment on the Federal Trade Commission's request for information on the use of Social Security Numbers (SSNs) in the private sector.

Founded in 1916, the American Financial Services Association (AFSA) represents approximately 360 non-traditional market-funded providers of financial services to consumers and small businesses. As adopted by our members, the mission of AFSA "is to assure a strong and healthy broad-based consumer lending services industry which is committed to: (1) providing the public with quality and cost effective service, (2) promoting a financial system that enhances competitiveness and (3) supporting the responsible delivery and use of credit and credit related products."

AFSA strongly supports the FTC's leadership role in the President's Identity Theft Task Force effort to combat identity theft. Financial institutions bear the burden of costs related to identity thefts when they occur as well as expenses intended to preempt the crime, such as reissuing credit and debit cards when merchant data is compromised. Each data compromise and identity theft event increases expenses to financial institutions and threatens to lower consumer confidence in the safety of the financial system. Securing sensitive customer data is a priority of every organization that retains that information.

Single Universal Identifier

The Social Security Number (SSN) is the only consistent and universally accepted form of identification used in commerce for purposes of verification, fraud prevention and recovery, consumer credit applications, employment security and screening and "business-to-business" transactions. Addresses and phone numbers can change many times in an individual's lifetime. Numerous American citizens share common names and birth dates with one another, and names are often changed upon marriage or other

circumstances. SSNs are integral to authenticating whether individuals are who they claim to be for the purposes of a variety of commercial transactions.

AFSA understands that any "alternative" unique identifier to SSNs would lower the value of SSN theft by identity thieves. But it is very important to recognize that any such alternative identifier will simply become the new target for identity thieves to acquire. Rather than reducing identity theft, the implementation of an "alternate SSN" would only create a new vehicle for identity theft. Any resolution of the current concerns about SSNs must focus on ID theft itself, not the form of ID that is being stolen.

In addressing the issue of stolen data, it is reasonable to surmise that if would-be thieves are sophisticated enough in their methods to acquire SSNs from government, academic and private entities, they will be sophisticated enough to acquire any alternative identifier for their use as well. Any discussion of a prohibition of government or private use of SSNs must take into consideration the overwhelming costs of such a conversion and the utter lack of progress any such conversion would make toward the real end of curbing identity theft.

Use of SSNs in Financial Services Industry

When considering the uses of the SSN in the financial services industry, it is critical to recognize that any universal unique identifier could serve for these purposes. Of course, if another identifier was adopted, then that would become the new target of identity thieves. This fact cannot be overlooked when considering the role of SSNs in identity theft and fraud prevention.

Legal Requirements

Businesses are required to collect and use SSNs in compliance with existing federal and state laws. Financial institutions use SSNs to comply with anti-money laundering (AML) laws, the Bank Secrecy Act, the USA Patriot Act and, along with child welfare enforcement and other laws regarding parents in arrears of child support payments (i.e., "Deadbeat Dad" laws). Title V of the Gramm Leach Bliley Act of 1999 requires financial entities to safeguard the security and confidentiality of customer information, including SSNs, and to protect against any threats or hazards to the integrity of sensitive personal information. Section 628 of the Fair Credit Reporting Act also sets requirements for proper disposal of information constituting or derived from customer reports.

Credit History for Underwriting Purposes

Financial services entities communicate regularly with consumer reporting agencies to properly match data to the correct file, allowing consumers to obtain benefits, such as credit and insurance. Consumer reporting agencies routinely receive literally billions of updates from more than 18,000 data furnishers, in addition to records from more than

30,000 public record sources, every month. They utilize sophisticated algorithms to ensure that the right information is loaded into the correct file, and the SSN is a vital piece of matching data employed for these purposes. Further, the SSN is used to help ensure that the correct file is delivered to the entity that requests it, and the SSN is also a vital piece of that data matching. The SSN is also necessary to ensure that credit information from a debtor is reported back to the bureau on the correct individual.

Businesses use SSNs to locate shareholders, beneficiaries and heirs, and owners of unclaimed goods for notification purposes. Financial institutions, attorneys, shipping companies, and many others may use SSNs to locate individuals when information, assets or lost or stolen items need to reach their owner.

Financial entities often use SSNs to audit and ensure the quality of services provided to customers by keeping track of all the products and services provided to a single individual within or across multiple lines of business. In addition, businesses use SSNs to locate parties to enforce contractual obligations on debtors. Credit-issuing retail stores, telecommunications companies and utility companies may use SSNs to locate subscribers with long-overdue payment obligations.

Fraud Control

Private companies rely on SSNs for identity verification and authentication purposes. AFSA believes that removing the SSN from the authentication process would make it a significantly easier task for thieves trying to impersonate their intended victims to commit account fraud or to open new accounts in their names. Financial institutions use databases to detect and prevent fraud, and the SSN plays a key role in helping these databases to match and confirm vital information.

Businesses use SSNs to locate potential victims upon discovery of fraudulent schemes. Financial institutions, for example, may all use SSNs to locate victims of fraud and ID theft to notify them to monitor or close certain accounts.

Finally, pursuant to the Fair and Accurate Credit Transactions Act (FACT Act), a number of federal agencies (including the FTC) have issued joint “Red Flag” guidelines that would require financial institutions to use SSNs to detect circumstances that may indicate identity theft or fraud.

Employees Verification

Companies in the private sector use the SSN throughout the employee application, payroll and tracking process. When individuals apply for a job, the company collects their SSN to verify their identity, check citizenship status, and run a criminal background check. Without the SSN, companies would have a less accurate method of ensuring that they are not hiring a convicted felon, fugitive from the law or an illegal alien to fill a job where such a background would prove troublesome. An example of this would be an individual with an embezzlement felony in his past applying for a job as CFO of a small

finance company. The finance company needs to know the applicant's background when deciding if they can be trusted to manage the company's accounts.

Organizations also use SSNs to conduct background checks on prospective volunteers. For example, youth groups might screen for volunteers in day care centers/schools to exclude pedophiles or bus drivers with alcohol & drug violations.

Businesses also use SSNs to locate former employees to administer retirement benefits such as a remaining 401(k) account or pension payments. If the individual does not update his address with their former employer, but is eligible to receive money from them, an SSN allows the company to conduct a credit search to find their latest address.

Once an individual is employed, businesses use the SSN to administer payroll information on the employee. The SSN helps companies identify employees with common names, track salary and benefit history, and report salary and benefits to the IRS.

Limits on Public Display and Availability

When focusing on lost data, AFSA does believe that the prohibition of display of SSNs on government forms or records that are publicly available – drivers licenses, state ID cards, tax forms, government checks or deeds – may lessen the risk of identity theft that results simply by these documents falling into the wrong hands. It must be recognized, however, that this possible slight reduction in opportunities for identity theft is more than offset by the difficulties now encountered in verifying that a public record such as a bankruptcy filing or a judgment does or does not attach to the actual person seeking to transact business with the financial services industry. This greatly decreases the efficiency of the marketplace and often times leads to unnecessary delays and frustrations.

Subject to the same objection as just stated in connection with SSNs in public records, AFSA also believes that reasonable restrictions on the display and public availability of SSNs by the private sector could be supported by our industry and readily implemented. Such restrictions could cover SSNs being required for online passwords and display on the internet, employee badges, health insurance cards or other means of identification that may be visible to other individuals. AFSA firmly believes, however, that any such restrictions should be only a suppression of the display of the SSN and not a prohibition of the use of the identifier.

In the ongoing study concerning SSNs in the public and private sector, and possible alternative identifiers and prohibitions on use, we ask the FTC to consider an evaluation of *benefits to consumers* that the responsible and legitimate use of SSNs brings. We would also ask the FTC to consider the societal costs on government, industry and consumers of replacing SSNs with any alternative. And finally, we ask the FTC to consider whether any alternative unique identifier would really achieve the end goal of

preventing, or even reducing, identity theft. Rather, would it not simply give thieves another piece of data to steal, thus making identity theft easier and the restoring of victims' credit files that much more difficult?

We point out that Title IV of the Gramm-Leach-Bliley Act (GLBA) already requires financial services companies to employ data security safeguards, a customer response program, and a comprehensive privacy policy. These security requirements are governed and monitored by an effective group of federal financial regulators who perform regular examinations of businesses under their jurisdiction. As a result of these safeguards, data thefts at financial institutions are a rarity in comparison to other industries.

We also point out the recent study by the Government Accountability Office (GAO) showing the link between data breaches and identity theft to be unclear. Of the 24 largest data breaches over the last six years, only three resulted in account fraud, while just one lead to the establishment of new accounts for fraudulent purposes. Financial services entities have strong incentive - both for risk and reputation management, as well as for legal compliance - to use the most effective technology available to safeguard the sensitive personal information they use. The track record of our industry, in comparison to retailers, healthcare, education and government agencies, shows us to be the leaders in data protection and identity theft prevention.

It would be worthwhile for the President's Identity Theft Task Force to review the GLBA data security standards and consider using them as a framework for non-financial institutions that use and collect SSNs. Where SSN usage by other industries cannot be efficiently reduced, its protections should be increased to the level already maintained by financial institutions.

AFSA appreciates the opportunity to continue working with the FTC and the President's Identity Theft Task Force. If you have any questions or would like to discuss the matter further, please contact Matt Gannon, AFSA Director of Federal Government Affairs, at

Sincerely,

Bill Himpler
Executive Vice President, Federal Affairs
American Financial Services Association